Europäisches Patentamt

European Patent Office

Office européen des brevets

(19)

(11)   **EP 0 762 340 A2**

(12)   **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
12.03.1997 Bulletin 1997/11

(51) Int Cl.⁶: **G07C 9/00, G06K 9/00**

(21) Application number: 96306267.4

(22) Date of filing: 29.08.1996

(84) Designated Contracting States:
DE FR GB IT NL

(30) Priority: 05.09.1995 US 523328
21.11.1995 US 561323

(71) Applicants:
- CANON KABUSHIKI KAISHA
  Tokyo (JP)
- Canon U.S.A. Inc.
  New York, NY 11042-1113 (US)

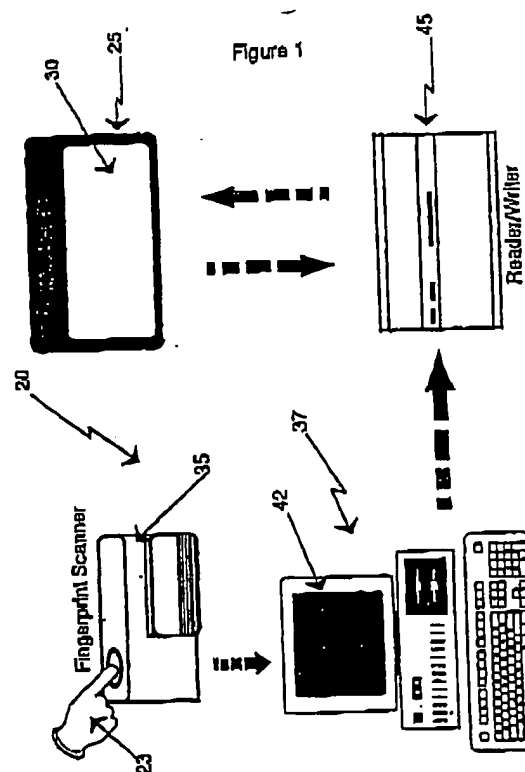(72) Inventor: Price-Francis, Stephen
Huntington, NY 11743 (US)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
2-5 Warwick Court
High Holborn
London WC1R 5DJ (GB)

(54)   **Biometric identification process and system**

(57)   A system for verifying that a card possessor is the authorized card owner compares scanned fingerprint data with fingerprint data encoded on an optical card. More than one of the person's fingerprints are encoded on the card, and the process of identification of the card possessor involves the random selection of separate fingerprints for scanning and comparison against the encoded fingerprints. A card reader/writer reads fingerprint characteristic information from an optical card inserted therein and a processing unit, connected to a fingerprint scanner and card reader/writer extracts from the scanned fingerprint certain well known indicators, and matches the recorded fingerprint characteristic data with the scanned fingerprint characteristics to establish identity therebetween.

Figure 1

EP 0 762 340 A2

Description

The present invention is generally related to a method and system for verifying the identity of a person, notably by comparing certain physical characteristics of the person, in one embodiment, the fingerprint of the person, with a recorded copy of information corresponding to the characteristics of that person provided on an optical card. In the present invention, the process of verifying the identity of the individual card owner involves the successive and sequential comparisons of one or more single characteristics, e.g., fingerprints, preferably randomly selected if more than one is required to verify the identity. This method of proceeding facilitates an identification of the individual while maintaining a higher degree of accuracy due to the possible use of higher degrees of correlation that those that are normally available when matching a single physical characteristic.

Currently, bank cards are used throughout the world which comprise one of more magnetic strips or other recording medium on or in the card, carrying coded information thereon. Although simple to use, there is no inherent means in the card for verifying that the person presenting the card is actually the true owner of the card. While in many circumstances a user, will input a Personal Identification Number (PIN) into a bank card machine, the level of security afforded is still not high, given that many users will write down a PIN number in a check book or the like, making the number easily accessible to a criminal.

There are other circumstances in which a verification of the identity of persons is necessary. Debit and Point-of-Sale cards are gaining the same popularity as credit cards. Welfare systems are investigating automatic distribution of benefits through a carded system. When businessmen travel between countries it is necessary to verify the identity of each person passing through customs and identify each as citizen, resident alien, permanent resident and the like. The identification must be accurate, but not too rigorous to be inconvenient. There are a number of possibilities for biometric identification including physical features, hand geometry, retinal scans, facial images, fingerprints and the like.

It has been proposed by many that the minute details of a person's fingerprint could be encoded (i.e., in binary coded form) into memory on a card. For example, a coded version of a fingerprint can be stored upon a card. When verification is required, it is necessary for the user to display his fingerprint to a scanner, and at the same time insert a card into a reader which extracts the coded information identifying the fingerprint, and with a processor, compare the authorized owner's fingerprint with the stored characteristics of the owner's fingerprint.

However, the accuracy of such systems is limited, since normally these systems only record some of the characteristics of a person's fingerprint on the card. And the environmental measurement conditions and posi-

tions must be matched as well. False rejections are very common on the single fingerprint identification systems. A rotated or rolled fingerprint, fingerprints taken or scanned with different pressures of the finger on the scanner while it is being scanned initially, dirt, a blemish or other injury on the finger being scanned, all are potential problems leading to false rejections. While conserving memory requirements, the accuracy of such methods, using only a single fingerprint, can be very low. The comparison of a single scanned finger with the corresponding recorded fingerprint information thereto, may incorrectly provide false rejections due to any of these conditions. For example, these systems do not account for temporal perturbations, e.g., a scraped, burned or cut finger, that may exist on the owner's finger, thereby giving rise to a false reading of the single fingerprint image.

The need to verify with accuracy the identity of a card owner is necessary in a wide variety of circumstances, including at a passport and immigration check, at banking and other financial systems, high security areas and the like. What is needed is a method making it more difficult for criminals to fraudulently use a stolen card and the like. As more and more accuracy is required the probability of false rejections increases. The need for a simple, more accurate method which facilitates the verification process is thus of increasing importance.

Accordingly, the present invention provides a method and system for verifying identification of a person with increased accuracy, while concomitantly, reducing the probability of false rejection for the authorized card owner.

The method includes the steps of comparing a scanned physical characteristic, such as a fingerprint, with recorded information corresponding to the scanned physical characteristic, e.g., a fingerprint, as known in the art, but goes beyond the state of the art by using a novel process of randomly and sequentially selecting more than one physical characteristic for scanning and comparison against recorded characteristic data, thus enhancing the accuracy of the individual identification process and reducing the probability of improper false rejections.

In this manner the invention can be used for persons temporarily disabled due to broken bones or to sprained muscles, paraplegic persons, persons who cannot provide a certain finger for scanning due to a recent accident, for example, or victims of intentional maiming or accidents who no longer possess a hand or have lost fingers. Furthermore, the invention accounts for a poor scan, resulting in an improper false rejection, for example, on a single fingerprint, or rejections due to injuries or to dirt or blemishes on the selected finger or the scanning equipment. The invention advantageously reduces the number of false rejections while at the same time enabling the use of a high comparison correlation to ensure a low number of false acceptances.

The system utilized by the method of the invention includes a storage medium, preferably portable, and more preferably an optical card, storing more than one characteristic, e.g., fingerprint, of the authorized card owner, a device for reading the stored characteristics, preferably a card reader/writer into which the card is inserted, or placed thereon, and which accesses the recorded characteristic data of the card owner, a scanner (reading means) for reading a selected physical characteristic, e.g., fingerprint of the card owner, and a Processing Unit (PU) for extracting essential characteristics of the scanned body part and comparing these characteristics with the recorded physical characteristics.

Potential applications of the invention include, for example, controlling entry at passport and immigration checkpoints, ensuring personal identification in financial transactions (e.g., credit card systems), and enhancing security at high security installations, and the like.

Therefore, it is an object of the present invention to provide a method that increases the accuracy of the security identification through the use of higher degrees of correlation.

It is another object of the invention to facilitate verification of identity by decreasing the probability of false rejections in the identification process of an authorized card owner, while not permitting unlawful use in attempting to circumvent personal data protection.

Another object of the invention is to provide an individual recognition system comprising: a storage medium storing as biometric data a plurality of physical characteristics of a user; reading means for extracting from the user biometric data representing one of the physical characteristics stored by the storage means; comparison means for determining whether or not the extracted biometric data represents the same physical characteristic as corresponding stored biometric data obtained from the storage medium; and control means for instructing the reading means to extract from the user additional biometric data representing a different physical characteristic stored by the storage means, depending on the determination by said comparison means.

Yet another object of the invention is to provide a personal identification method using a data storage medium containing previously stored biometric data representing a plurality of physical characteristics of a user, the method comprising: extracting from the user biometric data representing one of the physical characteristics stored by the storage medium; determining whether or not the extracted biometric data represents the same physical characteristics as corresponding stored biometric data obtained from the storage medium; and extracting from the user additional biometric data representing a different physical characteristic stored in the storage medium depending on the determination at the determining step.

Still another object of the invention is to provide an individual recognition system for use with a storage me-

dium on which biometric data corresponding to a plurality of physical characteristics of the user has been stored, the system comprising: reading means for extracting from the user biometric data representing one of the physical characteristics stored by the storage means; comparison means for determining whether or not the extracted biometric data represents the same physical characteristic as corresponding stored biometric data obtained from the storage medium; and control means for instructing the reading means to extract from the user additional biometric data representing a different physical characteristic stored by the storage medium, depending on the determination by the comparison means.

Other objects and features of the present invention will be apparent from the following detailed description of a number of embodiments of the invention, which are described by way of example only with reference to the accompanying drawings.

Figure 1 shows the system components for a preferred embodiment for carrying out the method of an embodiment of the invention.

Figure 2 represents the main stages of the method according to an embodiment of the invention in the form of a flowchart.

Figure 3 provides an example of the information, including a physical representation of the user's fingerprint, that might be printed on the front of the user's card, the reverse of which carries the coded fingerprint data as shown in Figure 1.

Figure 4 demonstrates the instructions to place the randomly selected finger and the Live Image Preview which might be obtained by the user following the instruction.

Figure 5 shows the resulting information which can be downloaded to the scanning station when the user's identity has been verified that can be displayed on the host CPU at a passport or immigration entry point.

Figure 1 shows an embodiment of a fingerprint identification system 20 for carrying out the method of the present invention. Using the system 20 of Figure 1, the fingerprints of the card owner 23 are stored on the encoded portion of an optical card 25, as part of individual identification information. As shown in Figure 3, the identity card 25 can also contain other various biometric and representative information about the individual card owner 23, recorded physically on the face of the card 28 or encoded thereon 29, or recorded on electronic or optical media 30, including, for example, name, account number, date of birth, sex, height, weight, information on citizenship, health inspection or health information and the like might be maintained. The optical card 25 also comprises memory 30 for storing the fingerprint data. Preferably, only certain characteristics of a plurality of fingerprints are stored on the card 25, thereby conserving memory space. The memory capacity can be reduced down to only about 1 Kbyte per fingerprint when only certain key characteristic features are encoded.

Such fingerprint characteristics are preferably limited to a few significant features such as the depth and interval of the fingerprint, ridge pattern information, or key features relating to the number and kind of vortices, arcs, crossings and other line forms shown by the fingerprints. However, it should be noted that optical cards with a large memory capacity are available, but it may be advisable for other reasons to limit the amount of data recorded therein (for example, correlation thereof would require the processing unit used with the present system to have excessive computational capacity). Extraction and matching software libraries (not shown) can be used of the type developed by The Phoenix Group, Inc. of Pittsburg, Kansas. However, the present invention works well with any fingerprint matching system.

In the present invention, data representing the characteristic features of a plurality of fingerprints, which may be all of the fingerprints or only a limited number of fingerprints from each hand of an authorized person, are preferably coded and stored on the card 25, in the form of a binary or multi-value coded signal. This is preferably done by scanning designated fingers of the person when issuing a card 25 on similar equipment 20 to that which will be used during verification. Any number of fingerprints may be chosen for scanning from one to all five fingers on each hand. Therefore, the card 25 storage mechanism 30 carries information relating to more than one finger of the person 23, as explained more fully below, so that the system can request alternative fingerprint information if one or more of the fingers are either not available of scanning, due to cuts, blemishes or other injury, or a defective fingerprint was originally taken or if a first or later scans fail to confirm the identify of the card holder.

Although the disclosed preferred embodiment has been described as utilizing fingerprint data, any biometric data representing a plurality of physical characteristics can be utilized. For example, retinal scans of both of a cardholder's eyes can be encoded onto the card. Similarly, palm prints of each of the cardholder's hands can also be used. In fact, the present invention is not limited to such obvious groupings of physical characteristics. For example, the left hand print, right eye retinal scan, and right hand fingerprints can all be stored on the optical card and randomly selected ones of the body parts corresponding to such characteristics required to be presented for verification. Biometric data representing other physical characteristics, such as the cardholder's signature (its appearance or characteristics of how the cardholder forms his signature), facial characteristics, or keyboard dynamics (such as keying pressure, rate, sequence, or the like) can also be compared.

The remaining components of Figure 1, 35, 37, 42, 45 will be described in relation to the flowchart, as depicted in Figure 2, showing the main steps when using the invention. The process of identification of the individual card owner 23 with the current invention is based upon the random measurement of successive and sequential single fingerprints, as opposed to the measurement of all fingerprints or merely the measurement of only a single fingerprint.

The process 45 strikes an acceptable balance between confirmation of the identity of the card holder 23 (a low number of false acceptances) with a facilitation or ease of use of the system 20 (a low number of false rejections). The balance is achieved with two basic components. Facilitation is achieved by the use of multiple (random) fingerprint comparisons. Therefore, if a problem, environmental or physical, impedes a first match, other fingers can be called for and scanned until a match is achieved. Thus a high correlation of fingerprint attributes can be required for a match, increasing the accuracy of the verification of the identity of the user. The random nature of requests for specific fingers on either or both hands further impedes criminal activity. Finally, preferably, after a predetermined number of attempts, a decision can be made to terminate the process with a rejection. The fact that a rejection occurs only after a predetermined number of unsuccessful comparisons advantageously results in a minimum of false rejections, while also allowing each individual comparison to utilize a high comparison correlation so that security is maximized.

Referring to the flow chart in Figure 2, to initiate 62 the process 45, the owner 23 inserts a card 25 into a card reader/writer 45. Preferably, either by a display 42 or some other means, the card owner is also requested to place 64 one of his or her fingers on the fingerprint scanner 35. In this instance, the particular hand and associated finger requested for scanning is random, as the result of any conventional random algorithm. The fingerprint scanner 35 can be any of a wide range of suitable scanners, such as those manufactured by Digital Biometrics, Inc. The scanner 35 comprises a fingerpress having a transparent section through which the fingerprint image can be obtained.

The scanner 35 reads an image 65 of the selected fingerprint of the user 66. Similar to the process of encoding the fingerprint characteristic data onto the card 25, described above, the scanning can be carried out using a number of techniques, e.g., optically using high intensity illumination and an array of photosensitive diodes as a camera to record an image, or some other optical scanning device such as a laser scanner, to provide an image which can be processed electronically.

The fingerprint pattern is converted to an electric signal 69 and sent to a peripheral PU 37 or to a PU 37 in the scanner 35 itself. In the preferred embodiment, the extraction and matching programs are stored in the memory of PU 37. Therefore, the fingerprint is transformed into an electronic signal which is coded into a binary or multi-value coded signal. Thereafter, certain characteristic patterns 75 are extracted preferably using the same extraction program as that used to encode the fingerprints. The extracted characteristics preferably correspond to those encoded onto the optical card. As

mentioned above, with reference to the card encoding process, such fingerprint characteristics are preferably significant features such as the depth and interval of the fingerprint, ridge pattern information, or key features relating to the number and kind of vortices, arcs, crossings and other line forms shown by the fingerprints. The characteristic extracted are used by the matching program for comparison with the fingerprint characteristic data encoded in the optical card.

As shown in Figure 2, the recorded data of the particular scanned fingerprint is accessed from the optical card 78 using an optical card reader 45 such as the RW-20 Reader/Writer manufactured by Canon Inc. of Japan. The card reader/writer 45 receives the recorded fingerprint characteristic information on the card owner corresponding to the scanned fingerprint. The card reader/writer 45 outputs the recorded fingerprint information to the PU 37. The PU 37 can display the scanned fingerprint 65, along with the directive 51 indicating which finger is to be/has been scanned.

The next step is the comparison of the recorded fingerprint data with the specific extracted characteristics from the scanned fingerprint using the matching program 82. The extraction and matching algorithms are preferably implemented into software stored by the PU 37. The comparison of the recorded data with the scanned fingerprint information can be made according to any of the conventional matching algorithms depending primarily on the characteristic features extracted from the fingerprint image.

If a predetermined correlation exists between the recorded fingerprint characteristic data and the scanned fingerprint extracted characteristics 92, a display associated with the PU 37 can either indicate the identification confirmation 101, or alternatively, a decision signal 125 can be sent from the PU 37 to an operational device (not shown) such as a door or gate for security situations, coded lights can flash or the result can be displayed on one or more screens. The decisional pass/fail signal 125 may also be transmitted back to the card reader/writer 45 to retain the card 78 in a failure to identify situation or optically or otherwise mark the card 78 to indicate border crossings, access to secured areas or other encoded records on the card 78. A remotely located display (not shown) may also indicate that a match has been found, and thereby confirm identification. Instead of indicating confirmation on a display, of course, the verification decision can also be indicated through illumination of a specified color of light or other expedient, such as the opening of a door or gate.

However, if no match has been found 110, instead of immediately denying entrance or access to or identification of the individual, as the case may be, the present invention allows for the successive and sequential placement of further fingers onto the fingerprint scanner 115. Therefore, by allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, envi-

ronmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for by the method of the present invention. As mentioned above, the optical card carries information preferably related to at least two fingers on each hand.

In the preferred embodiment, if there was not a positive match on the first fingerprint, another finger, preferably associated with the other hand and chosen at random, is requested to be placed onto the fingerprint scanner. This finger is scanned by the fingerprint scanner and the same process, disclosed above, and as shown in Figure 2, is commenced until a decision is made either indicating a match or the lack thereof.

If in the second scan there is no match, a third finger is randomly selected for scanning and measurement. If again there is no match with the third randomly selected finger 120, recognition of the individual carrying the optical card could be denied 125 or additional attempts to verify identification could be pursued.

This method of allowing multiple attempts facilitates use of the card 25 and verification of the identity of the individual, while the use of higher degrees of correlation assures that the security of accurate identification is not sacrificed. Therefore, the system 45 for use in the method of the invention preferably comprises a fingerprint scanner 35 to scan one or more fingers in successive and sequential order; a card reader/writer 45 for receiving recorded fingerprint characteristic information from an optical card 25 inserted therein on the user corresponding to the particular scanned finger(s); and a PU 37, connected to the fingerprint scanner 35 and card reader/writer 45, for creating a coded signal representing the characteristics of the scanned fingerprint, extracting from the scanned fingerprint certain well known indicators, and matching the recorded fingerprint characteristic data with the scanned fingerprint extracted characteristics to establish identity therebetween.

In addition to the fingerprint characteristics, the card can also contain other various biometric and representative information 28, 29 about the individual card owner, inscribed on the card or electronically or optically stored, including, for example, the name, bank account number, date of birth, sex, height, weight, etc., and specifically, for a passport, the recorded media can contain information on citizenship, health inspection and a complete catalog of travel history 130, all of which can be displayed 129, 130 on the PU 37 at any given location, as shown in the sample display 42 of Figure 3.

The present invention is useful in many applications. For example, a government may issue cards to be used by authorized recipients of various government services, such as health insurance, welfare benefits, social security benefits, driver's licenses, or the like. The present invention can be used to prevent imposters from receiving such services. In this context, it should be noted that biometric data representing physical characteristics of a plurality of persons, for example, a family, can

be stored on a single optical card whereby, for example, any member of a family qualifying for government services can present the card and be identified as a qualified recipient of such services.

In another embodiment of the present invention, the storage medium, rather than be portable, can exist at a fixed location along with storage media storing biometric data for a number of other persons. For example, at secured facilities in which a limited number of people (e. g., employees) routinely request access, the storage medium can be built into a main computer system as a series of secured memory locations. In such a system, an employee, for example, seeking access to the secured facility can have his identity verified without producing a card since the system can make the required comparison by requesting presentation of appropriate employee body parts for scanning and comparing biometric data extracted from the employee with biometric data representing physical characteristics of relating to the employee stored in the secured memory location. The same successive and sequential comparison method as has been described above can then be used to permit or deny access.

While the preferred embodiment of the present invention has been described, it should be appreciated that various modifications may be made by those skilled in the art without departing from the spirit and scope of the present invention. Accordingly, reference should be made to the claims that determine the scope of the invention.

Claims

1. An individual recognition system comprising:

    a storage medium storing as biometric data a plurality of physical characteristics of a user;
    reading means for extracting from the user biometric data representing one of the physical characteristics stored by said storage medium;
    comparison means for determining whether or not the extracted biometric data represents the same physical characteristic as corresponding stored biometric data obtained from said storage medium; and
    control means for instructing said reading means to extract from the user additional biometric data representing a different physical characteristic stored by said storage medium, depending on the determination by said comparison means.

2. A system according to Claim 1, wherein the reading means includes a display for requesting that the user present one of the user's body parts for extraction of the biometric data corresponding thereto.

3. A system according to Claim 2, wherein the body part is one of the user's fingers.

4. A system according to Claim 1, wherein the storage medium comprises a portable storage medium.

5. A system according to Claim 4, wherein the portable storage medium comprises an optical card.

6. A system according to Claim 1, wherein said comparison means outputs a positive comparison result if a match is found between the extracted biometric data and the corresponding stored biometric data.

7. A system according to a Claim 6, wherein the control means instructs said reading means to extract from the user additional biometric data if a positive result is not output by the comparison means.

8. A system according to Claim 5, wherein said comparison means includes an optical card scanner.

9. A system according to Claim 1, wherein said biometric data represents fingerprint data of a plurality of the user's fingers.

10. A system according to Claim 9, wherein said reading means comprises a fingerprint scanner.

11. A system according to Claim 1, wherein said reading means comprises a retinal scanner.

12. An individual recognition system comprising:

    a portable storage medium storing as biometric data a plurality of physical characteristics of a user;
    reading means for extracting from the user biometric data representing one of the physical characteristics stored by said storage medium;
    comparison means for determining whether or not the extracted biometric data represents the same physical characteristic as corresponding stored biometric data obtained from said storage medium and outputting a positive comparison result if a match occurs; and
    control means for instructing said reading means to extract from the user additional biometric data representing a different physical characteristic stored by said storage medium if said comparison means does not output a positive test result.

13. A system according to Claim 12, wherein the reading means includes a display for requesting that the user present one of the user's body parts for extraction of the biometric data corresponding thereto.

14. A system according to Claim 13, wherein the body part is one of the user's fingers.

15. A system according to Claim 12, wherein the portable storage medium comprises an optical card.

16. A system according to Claim 15, wherein said comparison means includes an optical card scanner.

17. A system according to Claim 16, wherein said biometric data represents fingerprint data of a plurality of the user's fingers.

18. A system according to Claim 17, wherein said reading means comprises a fingerprint scanner.

19. A system according to Claim 12, wherein said reading means comprises a retinal scanner.

20. A personal identification method using a data storage medium containing previously stored biometric data representing a plurality of physical characteristics of a user, the method comprising:

    a first extracting step of extracting from the user biometric data representing one of the physical characteristics stored by the storage medium; a determining step of determining whether or not the extracted biometric data represents the same physical characteristics as corresponding stored biometric data obtained from the storage medium; and a second extracting step of extracting from the user additional biometric data representing a different physical characteristic stored in the storage medium depending on the determination at said determining step.

21. A method according to Claim 20, wherein the first extracting step requests that the user present one of the user's body parts for extraction of the biometric data corresponding thereto.

22. A method according to Claim 21, wherein the body part is one of the user's fingers.

23. A method according to Claim 21, wherein the storage medium comprises a portable storage medium.

24. A method according to Claim 23, wherein the portable storage medium comprises an optical card.

25. A method according to Claim 21, wherein said determining step outputs a positive comparison result if a match is found between the extracted biometric data and the corresponding stored biometric data.

26. A method according to Claim 25, wherein the additional biometric data is extracted from the user if a positive result is not output at said determining step.

27. A method according to Claim 24, wherein said determining step is performed using an optical card scanner.

28. A method according to Claim 21, wherein the biometric data represents fingerprint data of a plurality of the user's fingers.

29. A method according to Claim 28, wherein said first extraction step uses a fingerprint scanner.

30. A method according to Claim 21, wherein said first extraction step uses a retinal scanner.

31. An optical card for use in a personal identification system which reads data provided by a user of the card representing one of a plurality of physical characteristics, determines whether or not the extracted biometric data represents the same physical characteristics as corresponding stored biometric data, and reads additional biometric data provided by the user representing a different physical characteristic depending on the determination, said optical card containing memory storing biometric data representing a plurality of physical characteristics of the user.

32. An optical card according to Claim 31, wherein the biometric data stored on the card comprises fingerprint data of a plurality of the user's fingers.

33. An optical card according to Claim 32, wherein the optical card further stores other biometric and representative information about the user in machine-readable and human-readable form.

34. An individual recognition system for use with an optical card on which biometric data corresponding to a plurality of physical characteristics of a user has been stored, said system comprising:

    reading means for extracting from the user biometric data representing one of the physical characteristics stored by the optical card; comparison means for determining whether or not the extracted biometric data represents the same physical characteristic as corresponding stored biometric data obtained from the optical card; and control means for instructing said reading means to extract from the user additional biometric data representing a different physical characteristic stored by the optical card, depending on the determination by said comparison means.

35. A method for identifying one person from a plurality of persons, said method comprising the steps of:

    gathering identification data from the plurality of persons;
    storing the gathered data; and
    providing apparatus for repeatedly obtaining different identification data from a person presenting himself or herself and comparing obtained identification data with stored data until the obtained identification data matches stored identification data.

36. A method according to claim 35, wherein the identification data gathered at said gathering step comprises biometric data representing fingerprints of each of the plurality of persons and is stored on one of a plurality of optical cards, and each of the plurality of optical cards is issued to the person whose identifying data it contains, for presentation by such person to establish his or her identity.

37. A method according to claim 35, wherein said method is adapted to determine which persons from a population of persons is a qualified person, said method further comprising a step of analyzing the gathered identification data to verify whether or not each of the plurality of persons from whom data has been gathered is qualified.

38. A method for biometrically verifying the identity of a card user, using a card, a card reader, a fingerprint scanner and a processing unit, the user carrying card onto which has been recorded fingerprint data into a memory of the card, the fingerprint data including specific characteristics of a plurality of fingerprints of the user comprising the following steps:

    successively and sequentially requiring each of a plurality of randomly selected fingers to be placed onto the fingerprint scanner until a match is found, the process comprising, for each fingerprint, the following steps:
    randomly selecting a finger of the user for placement onto the fingerprint scanner;
    scanning the randomly selected fingerprint of the user using the fingerprint scanner;
    generating an image of the scanned fingerprint of the user;
    converting the user fingerprint image to an electronic fingerprint signal;
    coding the electronic scanned fingerprint signal;
    extracting, from the coded scanned fingerprint signal, specific characteristics of the user fingerprint;
    accessing recorded fingerprint data of the user from the card reader by virtue of the manual

placement of the card onto or into the card reader;
    comparing, using the processing unit, the recorded fingerprint data with the specific extracted characteristics, a match being declared and identification confirmed if the recorded fingerprint data corresponds to the specific extracted characteristics of the scanned user fingerprint; whereby the use of more than one fingerprint facilitates higher degrees of correlation, assuring the highest level of security for accurate identification.

39. The method of claim 38, wherein the finger randomly selected for placement onto the fingerprint scanner must be one of a selected number of fingers on either hand.

40. The method of claim 38, wherein if no match is declared upon the scan of the first selected fingerprint, the method further comprises randomly selecting a finger on the other hand as the next successive and sequential finger for placement onto the fingerprint scanner to determine if a match is found.

41. A method for verifying that a card possessor is the authorized card owner through the recognition of fingerprint information, using an optical card, an optical card reader/writer, a fingerprint scanner and a central processing unit, the card possessor carrying an optical card onto which has been recorded authorized card owner fingerprint data, pertaining to the inner three fingers on each of the card owner's hands, into a memory of the card, the fingerprint data including specific characteristic features of the plurality of fingerprints of the card owner, comprising the following steps:

    inserting the card into the optical card reader/writer;
    randomly selecting one or more fingers of the card possessor for placement onto the fingerprint scanner, wherein the finger randomly selected for placement onto the fingerprint scanner must be one of the three inner fingers of either hand;
    successively and sequentially inserting a plurality of fingers onto the fingerprint scanner until a match is found, the process comprising, for each fingerprint, the following steps:
    scanning an image of a fingerprint of the card possessor on the fingerprint scanner;
    converting the scanned user fingerprint image to an electronic fingerprint signal;
    coding the electronic scanned fingerprint signal;
    extracting, from the coded scanned fingerprint signal, specific characteristics of the card pos-

sessor fingerprint;
accessing the recorded authorized fingerprint data of the card owner from the optical card reader by virtue of the manual placement of the card onto or into the optical card reader/writer;
comparing, using the central processing unit, the recorded authorized fingerprint data with the specific extracted characteristics, a match being declared and identification of the card possessor confirmed to be that of the card owner if the recorded authorized fingerprint data corresponds to the specific extracted characteristics of the scanned fingerprint;
whereby the use and random selection of more than one fingerprint facilitates higher degrees of correlation, assuring the highest level of security for accurate identification.

42. The method of claim 41, wherein if no match is declared upon the scan of the first selected fingerprint, the method further comprises randomly selecting a finger on the other hand as the next successive and sequential finger for placement onto the fingerprint scanner to determine if a match is found.

43. A method for biometrically verifying the identity of the holder of an identity card having a memory, using at least one fingerprint scanner, a card reader and a processing unit, the method comprising the following steps:

  scanning with a fingerprint scanner each of a plurality of fingers of the user;
  converting the plurality of fingerprint scans into a plurality of data signals each signal corresponding to data relating to a single fingerprint of the user;
  recording the fingerprint data of the user in the memory of the card;
  each verification of the identity of the card user requiring:
  placing the card into the card reader;
  successively and sequentially requiring each of a plurality of randomly selected fingers to be placed onto the fingerprint scanner until a match is found, the process comprising, for each fingerprint, the following steps:
  randomly selecting finger of the user for placement on the fingerprint scanner;
  scanning the randomly selected fingerprint of the user using the fingerprint scanner;
  converting the scanned image to a data signal corresponding to the fingerprint scanned;
  comparing the data signal of the randomly selected fingerprint with the fingerprint data on the card;
  signaling when a match has been achieved;
  whereby a comparison of a plurality of finger-

prints permits utilization of a higher correlation of similarity for each fingerprint compared while allowing a higher degree of successful identification because of the number of comparisons that are made.

44. The method of claim 43, wherein the step of randomly selecting a plurality of fingers of the user comprises randomly selecting each of the selected fingers from a single hand of the user.

45. The method of claim 43, wherein the step of randomly selecting a plurality of fingers of the user comprises randomly selecting each of the selected fingers from different hands of the user.

46. The method of claim 43, wherein the step of randomly selecting a plurality of fingers of the user comprises randomly selecting each of the selected fingers from different hands of the user and wherein each of the fingers successively and sequentially randomly selected are selected from alternate hands of the user.

47. The method of claim 43, wherein the step of successively selecting random fingers of the user comprises selecting all of the fingerprints of the user for comparison.

48. The method of claim 43, wherein the step of successively selecting random fingers of the user comprises selecting no more than three fingerprints from each hand of the user for comparison.

49. The method of claim 43, wherein the step of successively selecting random fingers of the user comprising selecting no more than three fingerprints for comparison.

50. The method of claim 43, wherein the step of successively selecting random fingers of the user comprising selecting the same three fingerprints from each hand of the user.

51. The method of claim 43, wherein the plurality of randomly selected fingers scanned is limited to a finite number of comparisons and if a match has not been achieved after the finite number of comparisons, the process further comprises generating a signal indicating that no match has been achieved.

52. The method of claim 51, wherein the plurality of attempts is limited to three randomly selected fingers which are scanned and compared.

53. The system of claim 43, wherein the card reader also comprises a card writer and wherein the method further comprises recording on the card data re-

17   EP 0 762 340 A2   18

lating to whether or not a match has been achieved.

54. The method of claim 43, wherein the card is an op-
    tical card and the card reader is an optical card
    reader and wherein the fingerprint data is optically   5
    recorded and read from the card.

55. The method of claim 43, wherein the method is used
    in a security system having a means for allowing
    access to a restricted area and wherein the method   10
    further comprises receiving a signal when a match
    has been achieved and permitting access to the se-
    cured area when a signal has been received indi-
    cating that the identity of the holder of the identity
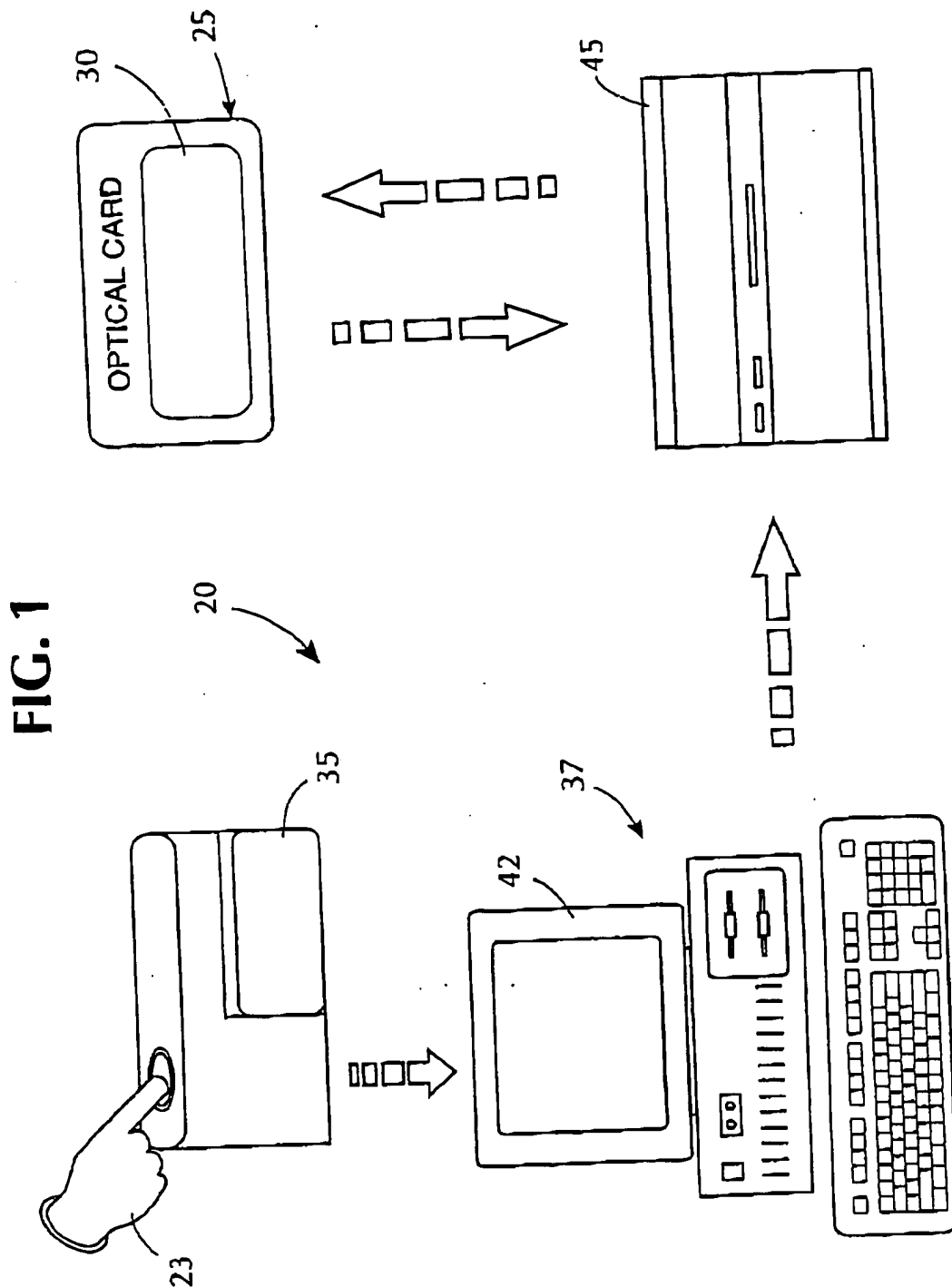   card has been verified.   15
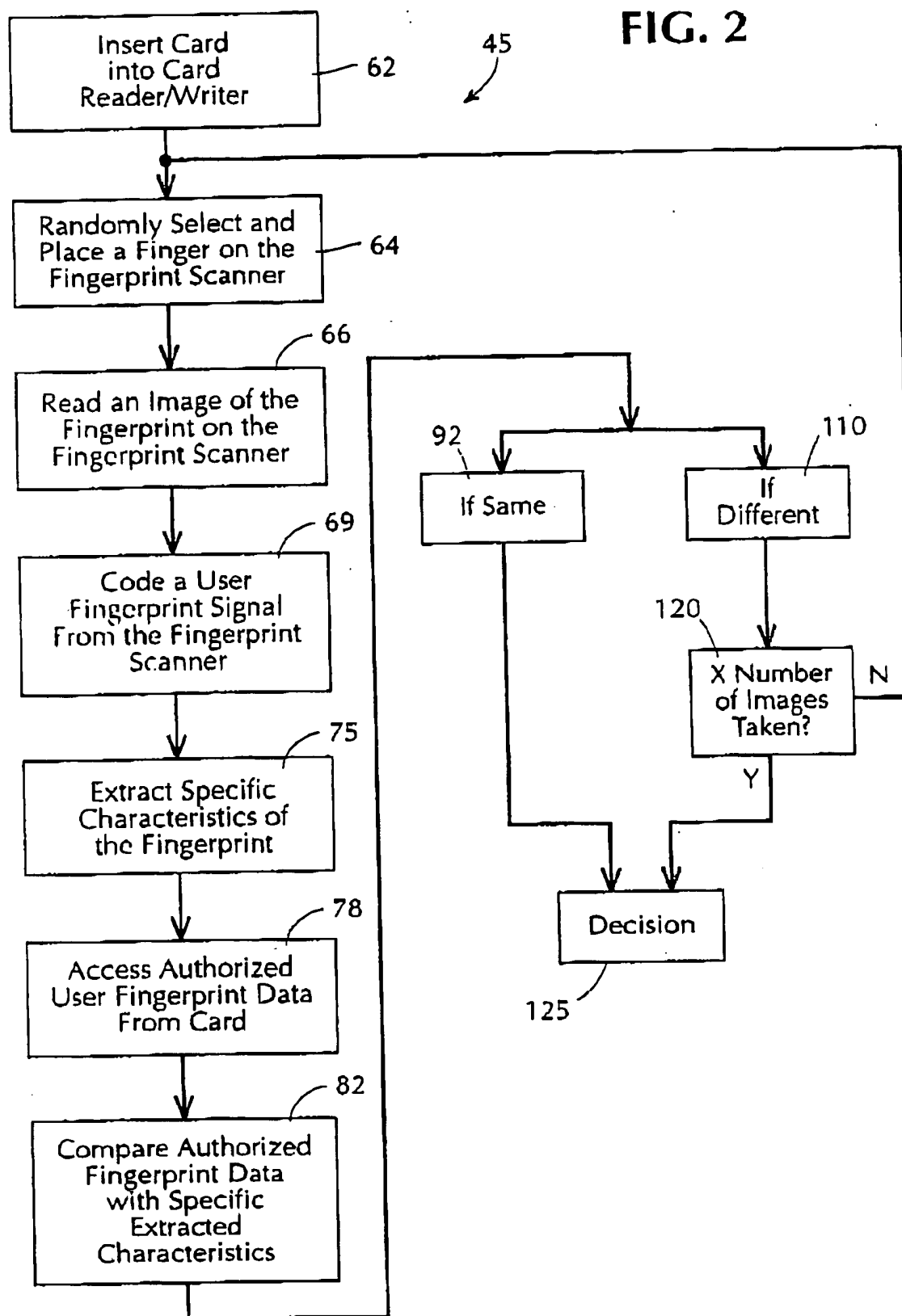
20

25

30

35

40

45

50

55

EP 0 762 340 A2

FIG. 1

FIG. 2

```
┌─────────────────┐
│   Insert Card    │
│   into Card      │──── 62        45
│  Reader/Writer   │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Randomly Select and│
│ Place a Finger on the│──── 64
│ Fingerprint Scanner │
└─────────────────┘
         │
         ▼                          66
┌─────────────────┐
│ Read an Image of the│
│ Fingerprint on the │
│ Fingerprint Scanner │
└─────────────────┘
         │
         ▼                          69
┌─────────────────┐
│  Code a User     │
│ Fingerprint Signal│
│ From the Fingerprint│
│    Scanner       │
└─────────────────┘
         │
         ▼                          75
┌─────────────────┐
│ Extract Specific │
│ Characteristics of│
│  the Fingerprint │
└─────────────────┘
         │
         ▼                          78
┌─────────────────┐
│ Access Authorized│
│ User Fingerprint Data│
│   From Card      │
└─────────────────┘
         │
         ▼                          82
┌─────────────────┐
│ Compare Authorized│
│ Fingerprint Data │
│  with Specific   │
│   Extracted      │
│ Characteristics  │
└─────────────────┘
```

```
          92                           110
  ┌──────────────┐              ┌──────────────┐
  │   If Same    │              │      If      │
  │              │              │  Different   │
  └──────────────┘              └──────────────┘
                                       │
                                 120   │
                          ┌──────────────┐
                          │  X Number    │   N
                          │  of Images   │
                          │   Taken?     │
                          └──────────────┘
                                  │ Y
                    ┌──────────────┐
                    │   Decision   │
                    └──────────────┘
                         125
```

FIG. 3

CITIZENSHIP AND IMMIGRATION

PEARSON INTERNATIONAL

- Evidence of Citizenship
- Passports | Application
- Visa | Carnet
- Biometric Information
- Entry GRANTED
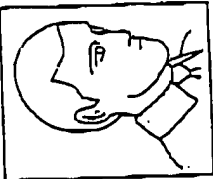
Name	Steve Cilic	
Date of Birth	April 12 1	Sex	Male
Height	5'10"	Hair Colour	Brown
Weight		Eye Colour	Green
Passport#	AP749856	Copies	1
Issued	August 13 199	At:	Toronto

Print History

129
42
130
101

Travel History

Non-Resident

- Entry GRANTED
- Cleared 90 Days
- Entry DENIED
- Health Inspection
- Eject Optical Card
- Exit to System

Date	Time	Port of Entry	Result
12-13-199	14:43:27	PEARSON	Entry - Granted
12-12-199	14:05:50	PEARSON	Entry - Granted
12-01-199	17:24:22	J.F. Kennedy	Entry - Granted
11-30-199	21:34:04	J.F. Kennedy	Entry - Granted
11-22-199	13:55:36	Houston Tex	Entry - Granted
11-22-199	13:01:37	J.F. Kennedy	Entry - Granted
11-21-199	18:41:04	J.F. Kennedy	Entry - Granted
10-19-199	17:58:27	PEARSON	Entry - Granted
10-17-199	14:08:43	FORT ERIE ONTARIO	Health Inspection
10-13-199	18:24:42	PEARSON	Cleared

EP 0 762 340 A2

FIG. 4

CITIZENSHIP AND IMMIGRATION

PEARSON INTERNATIONAL

Name   Steve Cilic
Date of Birth   April 12 1
Sex   Male
Brown
Green
1
Toronto

Evidence of Citizenship
Passports   Application
Visa   Carnet
Biometric Information
Entry GRANTED

Live Image Preview

Please place your right ring finger on the scanner

OK   Cancel

Non-Resident
Entry GRANTED
Cleared 90 Days
Entry DENIED
Health Inspection

Eject Optical Card

Exit to System

nt History

Granted
Granted
Granted
Granted
Granted
Granted
Granted

Entry - Granted   Health Inspection

10-19-199   17:58:27   PEARSON
10-17-199   14:08:43   FORT ERIE ONTARIO
10-13-199   18:24:42   PEARSON   Cleared

42
129
130
51
65
101

EP 0 762 340 A2

FIG. 5

TRAVEL DOCUMENT / DOCUMENT DE VOYAGE

NAME/NOM
STEVENSON, PETER

DOB/DDN
02 APR 1961

SEX
M

NAT
CDN

DOC. No/No DU DOC.
D23145890

EXPIRY/EXPIRATION
21 JAN 1996

D23145890 199601210

SIGNATURE
Peter Stevenson

IDCDNL1097022219Q1ZBIETQM3TYDM7
6104021M9503289CAN0160017910007
STEVENSON<<PETER<<<<<<<<<<<<<<<

(12)   **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
    28.01.1998 Bulletin 1998/05

(51) Int Cl.⁶: **G07C 9/00, G06K 9/00**

(43) Date of publication A2:
    12.03.1997 Bulletin 1997/11

(21) Application number: 96306267.4

(22) Date of filing: 29.08.1996

(84) Designated Contracting States:
    DE FR GB IT NL

(30) Priority: 05.09.1995 US 523328
                21.11.1995 US 561323

(71) Applicants:
    • CANON KABUSHIKI KAISHA
      Tokyo (JP)
    • Canon U.S.A. Inc.
      New York, NY 11042-1113 (US)

(72) Inventor: Price-Francis, Stephen
    Huntington, NY 11743 (US)

(74) Representative:
    Beresford, Keith Denis Lewis et al
    BERESFORD & Co.
    2-5 Warwick Court
    High Holborn
    London WC1R 5DJ (GB)
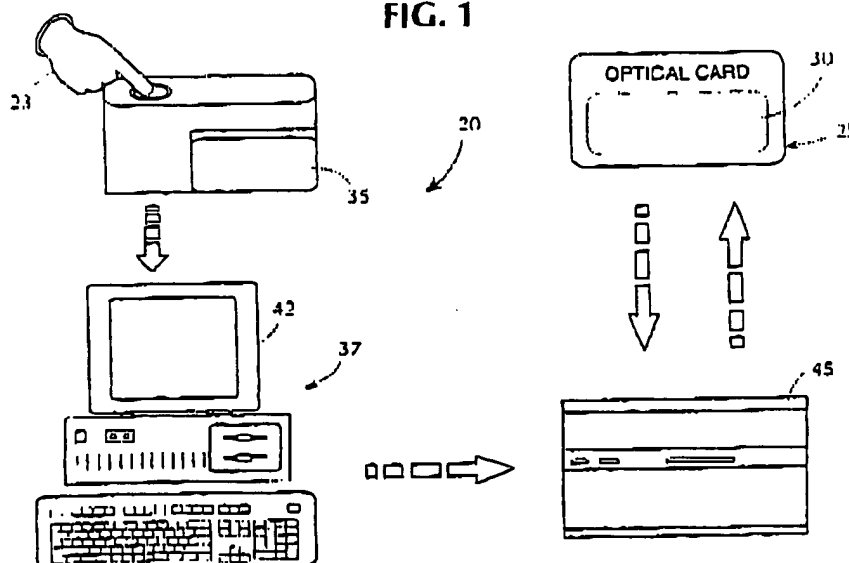
(54)   **Biometric identification process and system**

(57)   A system for verifying that a card possessor is the authorized card owner compares scanned fingerprint data with fingerprint data encoded on an optical card. More than one of the person's fingerprints are encoded on the card, and the process of identification of the card possessor involves the random selection of separate fingerprints for scanning and comparison against the encoded fingerprints. A card reader/writer reads fingerprint characteristic information from an optical card inserted therein and a processing unit, connected to a fingerprint scanner and card reader/writer extracts from the scanned fingerprint certain well known indicators, and matches the recorded fingerprint characteristic data with the scanned fingerprint characteristics to establish identity therebetween.

FIG. 1

EP 0 762 340 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 96 30 6267

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 4 993 068 A (PIOSENKA GERALD V ET AL)	1-6,8, 11,12, 15,16, 19-25, 27,30, 31,34-37	G07C9/00 G06K9/00
	* abstract; claims; figures * * column 4, line 30 - column 6, line 54 * * column 7, line 37 - column 10, line 11 *		
Y		7,9,10, 13,14, 17,18, 26,28, 29,32, 33, 38-52, 54,55	
X	US 4 151 512 A (RIGANATI JOHN P ET AL) * abstract; claims; figures * * column 6, line 25 - column 7, line 52 *	1	
Y		9,10,17, 18,26, 28,29, 32,33, 38-52, 54,55	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G07C G07F G06K
X	FR 2 634 570 A (REITTER RENAUD ;ANDRE CATHERINE (FR); REVILLET MARIE JOSEPHE (FR)) * abstract; claims; figures * * page 5, line 23 - page 8, line 19 *	1	
Y		7,13,14	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 December 1997	Meyl, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EP 0 762 340 A3

	European Patent Office	EUROPEAN SEARCH REPORT	Application Number EP 96 30 6267

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	WO 95 02225 A (BEHNKE ALFONS) * abstract; claims; figures * * page 2, line 14 - page 4, line 6 *	1-4,6, 12, 20-23, 25-29, 31,34, 35,38, 41-55	
A	EP 0 504 616 A (ASCOM AUTELCA AG) * abstract; claims; figures * * column 3, line 46 - column 4, line 6 *	1-4,12, 20,34, 35,38, 39,41, 43-55	
A	EP 0 010 611 A (SIEMENS AG)		
A	FR 2 585 153 A (DESGORCES JEAN)		TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 December 1997	Meyl, D

3